

C L A I M S

What Is Claimed Is:

5

1. A secret key generation method for generating secret keys to be sent from a center to entities, comprising the step of:

generating said secret keys peculiar to said
10 entities using pieces of information resulting from division of information specifying each of said entities.

2. An encryption method for use in a system in which a center sends to entities secret keys peculiar to
15 the entities respectively, and each entity uses a secret key peculiar to itself that has been sent from the center when it encrypts plaintext to ciphertext, the encryption method comprising the steps of:

generating said secret keys peculiar to said
20 entities using pieces of information resulting from division of information specifying each of said entities;
and

encrypting plaintext to ciphertext using a common key generated using a component contained in the secret
25 key peculiar to an entity that is a sender of the ciphertext, the component corresponding to one or more

pieces of information specifying another entity that is a destination of the ciphertext.

3. A cryptographic communications method for
5 communications of information between entities wherein a plurality of centers are provided, each of which generates secret keys peculiar to the entities using divided pieces of information resulting from division of information specifying each of the entities; one entity
10 generates a first common key using a first component contained in secret keys peculiar to the one entity sent from the centers, encrypts plaintext to ciphertext using the first common key and sends the ciphertext to another entity, the first component corresponding to one or more
15 of the divided pieces of information specifying said another entity; and said another entity generates a second common key identical to the first common key using a second component contained in secret keys peculiar to the another entity sent from said centers, and decrypts
20 said ciphertext to the original plaintext using the second common key, the second component corresponding to one or more of the divided pieces of information specifying the one entity.

25 4. A cryptographic communications method for communicating information between entities wherein:

secret keys peculiar to said entities are sent from a center to said entities;

one entity encrypts plaintext to ciphertext using a first common key derived from a first secret key peculiar
5 to the one entity sent from said center and sends the ciphertext to another entity;

said another entity decrypts said ciphertext to the original plaintext using a second common key identical to the first common key, the second common key being derived
10 from a second secret key peculiar to said another entity sent from said center, characterized in that;

a plurality of said centers are deployed;

each of said plurality of centers generates secret keys peculiar to said entities by adding random numbers
15 peculiar to said entities to divided pieces of information resulting from division of information specifying each of said entities; and

each of said entities generates a common key using a component, contained in the secret key peculiar to that
20 selfsame entity, corresponding to one or more of the divided pieces of information specifying an opposite entity.

5. The cryptographic communications method
25 according to claim 4, wherein computation formulas for generating secret keys at said centers are as follows:

$$\begin{aligned}
 \overrightarrow{S_{i1}} &\equiv g^{\alpha_{i1}H_1} [\overrightarrow{I_{i1}}] \pmod{P} \\
 \overrightarrow{S_{i2}} &\equiv \alpha_{i2} H_2 [\overrightarrow{I_{i2}}] \pmod{P-1} \\
 &\vdots \\
 \overrightarrow{S_{iK}} &\equiv \alpha_{iK} H_K [\overrightarrow{I_{iK}}] \pmod{P-1}
 \end{aligned}$$

5

where

vector s_{ij} is a secret key corresponding to j'th
 piece of divided information specifying
 entity i ($j = 1, 2, \dots, K$)

10

[vector I_{ij}] is j'th piece of divided information
 specifying entity i;

P is a prime number;

K is number of divisions in the information
 specifying entity i;

15

g is primitive element for GF (P);

H_j is a symmetrical $2^M \times 2^M$ matrix made up of
 random numbers;

M is size of divisions in the information
 specifying entity i; and

20

α_{ij} is a personal secret random number for
 entity i (where $\alpha_{i1} \dots \alpha_{iK} \equiv 1 \pmod{P-1}$).

6. The cryptographic communications method
 25 according to claim 5, wherein computation formulas for
 generating common keys at said entities are as follows:

$$\begin{aligned}
 K_{im} &\equiv \overrightarrow{S_{i1}} [\overrightarrow{I_{m1}}] \overrightarrow{S_{i2}} [\overrightarrow{I_{m2}}] \cdots \overrightarrow{S_{iK}} [\overrightarrow{I_{mK}}] \\
 &\equiv g^{\alpha_{i1} \cdots \alpha_{iK}} H_1[\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] \cdots H_K[\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] \\
 &\equiv g^{H_1[\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] \cdots H_K[\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]} \pmod{P}
 \end{aligned}$$

where

5 K_{im} is common key generated by one entity i for
another entity m ; and

vector s_{ij} [vector I_{ij}] is a component contained
in secret key vector s_{ij} of entity i ,
corresponding to divided piece of

10 information specifying entity m .

7. A common key generator provided at entities in
a cryptographic communications system for generating
common keys to be used in processing to encrypt plaintext
15 into ciphertext and in processing to decrypt ciphertext
into plaintext, comprising:

storage means at each entity for storing secret keys
peculiar to each respective entity produced for
respective pieces of information resulting from division
20 of information specifying each of said respective
entities;

selection means for selecting components
corresponding to pieces of information specifying
opposite entities to be communicated with, from among the
25 secret keys stored; and

means for generating said common keys using said components so selected.

8. A cryptographic communications system for
5 reciprocally performing, between a plurality of entities,
encrypting processing for encrypting plaintext that is
information to be sent into ciphertext and decrypting
processing for decrypting ciphertext so sent back into
original plaintext; comprising:

10 a plurality of centers that generate secret keys
peculiar to said entities using pieces of information
resulting from division of information specifying each of
said entities and that sends said secret keys to said
entities; and

15 a plurality of entities each of which generates a
common key employed mutually in said encryption and
decryption processing when communicating with another
entity, using a component contained in own secret key
sent from the centers, the component corresponding to one
20 or more pieces of information specifying said another
entity.

9. A computer readable recording medium that
stores a program that generates at entities involved in
25 communications common keys used in processing to encrypt
plaintext to ciphertext and in processing to decrypt said

ciphertext to said plaintext in a cryptographic communications system, comprising:

first program code means for causing said computer to select a component corresponding to one or more of
5 divided pieces of information specifying one entity from a secret key peculiar to another entity; and

second program code means for causing said computer to generate said common keys using said components selected.

10

10. An encryption method comprising the steps of:

generating a first secret key peculiar to ciphertext sending entity using first divided specifying information and a second secret key peculiar to ciphertext receiving entity using second divided specifying information, the first divided specifying information being obtained by dividing specifying information of the ciphertext sending entity into a plurality of blocks and the second divided specifying information being obtained by dividing specifying information of the ciphertext receiving entity into a plurality of blocks;

generating a common key using a component contained in the first secret key, the component corresponding to second divided specifying information of the ciphertext receiving entity, the common key having a structure of at

least three layers and an exponent portion of the common key having a multi-layer structure; and

encrypting plaintext to ciphertext using the common key.

5

11. A secret key generation method comprising the step of:

generating secret keys peculiar to entities using divided specifying information resulting from division of information specifying said entities into a plurality of blocks; and wherein

secret key for a first block of divided specifying information has a multi-layer structure; and

each of secret keys for remaining blocks of divided specifying information has a single-layer structure.

12. An encryption method comprising the steps of:

generating secret keys peculiar to entities using divided specifying information resulting from division of information specifying said entities into a plurality of blocks; and

encrypting plaintext to ciphertext at one entity using a common key generated using a component contained in the secret key peculiar to the one entity, the component corresponding to divided specifying information

for another entity to which said ciphertext is to be sent,
and wherein

secret key for first block of divided specifying
information has a multi-layer structure; and

5 each of secret keys for remaining blocks of divided
specifying information has a single-layer structure.

13. A cryptographic communications method for
communications of information between entities wherein a
10 plurality of centers are provided, each of which
generates secret keys peculiar to the entities using
divided specifying information resulting from division of
information specifying each of the entities into a
plurality of blocks; one entity generates a first common
15 key using a first component contained in secret keys
peculiar to the one entity sent from the centers,
encrypts plaintext to ciphertext using the first common
key and sends the ciphertext to another entity, the first
component corresponding to one or more of the divided
20 pieces of information specifying said another entity; and
said another entity generates a second common key
identical to the first common key using a second
component contained in secret keys peculiar to the
another entity sent from said centers, and decrypts said
25 ciphertext to the original plaintext using the second
common key, the second component corresponding to one or

more of the divided pieces of information specifying the one entity; secret keys for first block of divided specifying information have a multi-layer structure; and secret keys for remaining blocks of divided specifying
5 information have a single-layer structure.

14. A secret key generation method for generating secret keys peculiar to entities using divided specifying information resulting from division of information
10 specifying said entities into a plurality of blocks,
wherein:

computation formulas for generating said secret keys are as follows:

$$\overrightarrow{S_{i1}} = \alpha_i H_1[\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2[\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{S_{ij}} = \alpha_i H_j[\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$

$$\vdots$$

$$\overrightarrow{S_{iK}} = \alpha_i H_K[\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}} \overrightarrow{1} \pmod{N}$$

$$20 \quad \overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}} \overrightarrow{S_{i1}} \pmod{N}$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i1}} >^2 \pmod{N}$$

$$\vdots$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i1}} >^t \pmod{N}$$

$$\vdots$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i1}} >^T \pmod{N}$$

25 where

vector s_{ij} is a secret key corresponding to j'th

divided specifying information for entity
i (j = 1, 2, ..., K)
[vector I_{ij}] is j'th divided specifying
information for entity i;
5 vector l is a vector of dimension K wherein all
components are 1;
 H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of
random numbers;
 M_j is size of j'th divided specifying
10 information for entity i;
K is number of block divisions in information
specifying entity i;
 α_i is a personal secret random number for entity
i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is
15 Carmichael function);
 N is such that $N = PQ$ (where P and Q are
prime);
 β_{ij} is a personal secret random number for
entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{ik} =$
20 $\lambda(N)$);
 g is maximum generating element with modulo N;
vector g_{it} is a secret key for 1st block of
specifying information for entity i ($t = 0,$
25 $1, 2, \dots, T$);
 T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes
represented in (i) and (ii) below, then the
expressions $B = c^A$ and $B = \langle A \rangle^c$ represent (iii)
and (iv) below, respectively.

5

(i) $A = (a_{\mu\nu})$

(ii) $B = (b_{\mu\nu})$

10

(iii) $b_{\mu\nu} = c^{a_{\mu\nu}}$

(iv) $b_{\mu\nu} = a_{\mu\nu}^c$

15

15. An encryption method wherein:

secret keys peculiar to entities are generated using divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks;

20

plaintext is encrypted to ciphertext at one entity using a common key generated using a component contained in the secret key peculiar to the one entity, the component corresponding to divided specifying information for another entity that is a destination of said 25 ciphertext; and

computation formulas for generating said secret keys peculiar to said entities are as follows:

$$\overrightarrow{S_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

$$\begin{aligned}
 \overrightarrow{S_{ij}} &= \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1} \\
 \overrightarrow{S_{iK}} &= \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1} \\
 \overrightarrow{g_{i0}} &\equiv g^{\alpha_i^{-T}} \overrightarrow{1} \pmod{N} \\
 \overrightarrow{g_{i1}} &\equiv g^{\alpha_i^{-T}} \overrightarrow{S_{i1}} \pmod{N} \\
 5 \quad \overrightarrow{g_{i2}} &\equiv g^{\alpha_i^{-T}} \langle \overrightarrow{S_{i1}} \rangle^2 \pmod{N} \\
 \vdots \\
 \overrightarrow{g_{it}} &\equiv g^{\alpha_i^{-T}} \langle \overrightarrow{S_{i1}} \rangle^t \pmod{N} \\
 \overrightarrow{g_{iT}} &\equiv g^{\alpha_i^{-T}} \langle \overrightarrow{S_{i1}} \rangle^T \pmod{N}
 \end{aligned}$$

where

- 10 vector $\overrightarrow{s_{ij}}$ is a secret key corresponding to j'th divided specifying information for entity i ($j = 1, 2, \dots, K$);
- [vector $\overrightarrow{I_{ij}}$] is j'th divided specifying information for entity i;
- 15 vector $\overrightarrow{1}$ is a vector of dimension K wherein all components are 1;
- H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of random numbers;
- M_j is size of j'th divided specifying information for entity i;
- 20 K is number of block divisions in information specifying entity i;
- α_i is a personal secret random number for entity i
- 25 (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is

Carmichael function);
N is such that N = PQ (where P and Q are
prime);
β_{ij} is a personal secret random number for
5 entity i
(where β_{i1} + β_{i2} + ... + β_{iK} = λ(N));
g is maximum generating element with modulo N;
vector g_{it} is a secret key for 1st block of
specifying information for entity i (t = 0,
10 1, 2, ..., T);
T is degree of exponent portion; and
if c is a scalar, and A and B are matrixes
represented in (i) and (ii) below, the
expressions B = c^A and B = <A>^c represent (iii)
15 and (iv) below, respectively.

- (i) A = (a_{μν})
20 (ii) B = (b_{μν})
(iii) b_{μν} = c^{a_{μν}}
(iv) b_{μν} = a_{μν}^c

25
16. The encryption method according to claim 15,
wherein computation formulas for generating said common
keys are as follows:

30 $\overrightarrow{g_{0im}} = \overrightarrow{g_{i0}} [\overrightarrow{I_{m1}}]$

$$\begin{aligned}
 g_{1im} &= \overrightarrow{g}_{it} [I_{m1}] \\
 g_{tim} &= \overrightarrow{g}_{it} [I_{m1}] \\
 g_{Tim} &= \overrightarrow{g}_{iT} [I_{m1}] \\
 x_{1im} &= \overrightarrow{s}_{i2} [I_{m2}] \\
 x_{jim} &= \overrightarrow{s}_{ij} [I_{mj}] \\
 x_{kim} &= \overrightarrow{s}_{iK} [I_{mK}]
 \end{aligned}$$

5

$$\begin{aligned}
 K_{im} &\equiv \prod_{t=0}^T g_{tim}^{T-t} y_{im}^{(T-t)} \\
 &\equiv g_i^{-T} \sum_{t=0}^T C x_{1im}^t y_{im}^{T-t} \\
 &\equiv g_i^{-T} (x_{1im} + y_{im})^T \\
 &\equiv g_i^{-T} (x_{1im} + \dots + x_{kim})^T \\
 &\equiv g_i^{-T} (\alpha_i H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] + \beta_{iK})^T \\
 &\equiv g_i^{-T} (\alpha_i H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]) + \lambda N)^T \\
 &\equiv g_i^{-T} (\alpha_i H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}])^T \\
 &\equiv g_i^{-T} (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}])^T \pmod{N}
 \end{aligned}$$

10

15

where

g_{tim} (= vector \overrightarrow{g}_{it} [vector I_{m1}]) is a component corresponding to vector I_{m1} for entity m , selected from own vector \overrightarrow{g}_{it} for 1st block of information specifying entity i ($t = 0, 1, 2, \dots, T$);

20

x_{1im} = vector \overrightarrow{s}_{i1} [vector I_{m1}];
 x_{jim} (= vector \overrightarrow{s}_{ij} [vector I_{mj}]) is a component corresponding to vector I_{mj} for entity m , selected from own vector \overrightarrow{s}_{ij} for j 'th block of information specifying entity i ($j = 2, 3, \dots, K$);

25

K_{im} is a common key generated by one entity i
for another entity m; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3,$
 \dots, K), that is, $y_{im} = x_{2im} + x_{3im} + \dots +$

5 $x_{Kim}.$

17. A cryptographic communications method for
communications of information between entities, wherein

a plurality of centers are deployed, each of which
10 generates secret keys peculiar to said entities using
divided specifying information resulting from division of
information specifying each of said entities into a
plurality of blocks, and sends the secret keys to the
entities respectively;

15 one entity generates a first common key using a
first component contained in secret keys peculiar to the
one entity sent from the centers, encrypts plaintext to
ciphertext using the first common key, and sends the
ciphertext to said another entity, the first component
20 corresponding to divided specifying information for
another entity;

said another entity generates a second common key
identical to the first common key using a second
component contained in secret keys peculiar to said
25 another entity sent from the centers, and decrypts said
ciphertext using the second common key, the second

component corresponding to divided specifying information
for the one entity; and

computation formulas for generating said secret keys
at said centers are as follows:

$$\begin{aligned} 5 \quad \overrightarrow{S_{i1}} &= \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1} \\ \overrightarrow{S_{i2}} &= \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1} \\ \overrightarrow{S_{ij}} &= \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1} \\ \overrightarrow{S_{iK}} &= \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1} \end{aligned}$$

$$\begin{aligned} 10 \quad \overrightarrow{g_{i0}} &\equiv g^{\alpha_i^{-T}} \overrightarrow{1} \pmod{N} \\ \overrightarrow{g_{i1}} &\equiv g^{\alpha_i^{-T}} \overrightarrow{S_{i1}} \pmod{N} \\ \overrightarrow{g_{i2}} &\equiv g^{\alpha_i^{-T}} \langle \overrightarrow{S_{i1}} \rangle^2 \pmod{N} \\ \overrightarrow{g_{it}} &\equiv g^{\alpha_i^{-T}} \langle \overrightarrow{S_{i1}} \rangle^t \pmod{N} \\ \overrightarrow{g_{iT}} &\equiv g^{\alpha_i^{-T}} \langle \overrightarrow{S_{i1}} \rangle^T \pmod{N} \end{aligned}$$

15 where

vector $\overrightarrow{s_{ij}}$ is a secret key corresponding to j'th
divided specifying information for entity
 i ($j = 1, 2, \dots, K$)

[vector $\overrightarrow{I_{ij}}$] is j'th divided specifying
information for entity i ;

20 vector $\overrightarrow{1}$ is a vector of dimension K wherein all
components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of
random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

5 α_i is a personal secret random number for entity i (where gcd (α_i, λ(N)) = 1 and λ(·) is Carmichael function);

N is such that N = PQ (where P and Q are prime);

10 β_{ij} is a personal secret random number for entity i (where β_{i1} + β_{i2} + ... + β_{iK} = λ(N));

g is maximum generating element with modulo N;

vector g_{it} is a secret key for 1st block of

15 information specifying entity i (t = 0, 1, 2, ..., T);

T is degree of exponent portion; and

if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the

20 expressions B = c^A and B = <A>^c represent (iii) and (iv) below, respectively.

(i) A = (a_{μν})

25 (ii) B = (b_{μν})

(iii) b_{μν} = c^{a_{μν}}

(iv) b_{μν} = a_{μν}^c

18. The cryptographic communications method according to claim 17, wherein computation formulas for 5 generating said common keys are as follows:

$$g_{0im} = \overrightarrow{g}_{i0} [\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g}_{i1} [\overrightarrow{I_{m1}}]$$

$$g_{tim} = \overrightarrow{g}_{it} [\overrightarrow{I_{m1}}]$$

$$g_{Tim} = \overrightarrow{g}_{iT} [\overrightarrow{I_{m1}}]$$

$$10 \quad x_{2im} = \overrightarrow{s}_{i2} [\overrightarrow{I_{m2}}]$$

$$x_{jim} = \overrightarrow{s}_{ij} [\overrightarrow{I_{mj}}]$$

$$x_{Kim} = \overrightarrow{s}_{iK} [\overrightarrow{I_{mK}}]$$

$$15 \quad K_{im} \equiv \prod_{t=0}^T g_{tim}^{T-C_t y_{im}^{(T-t)}}$$

$$\equiv g^{\bar{\alpha}_i^T} \sum_{t=0}^T C_{tim} x_{1im}^t y_{im}^{T-t}$$

$$\equiv g^{\bar{\alpha}_i^T} (x_{1im} + y_{im})^T$$

$$\equiv g^{\bar{\alpha}_i^T} (x_{1im} + \dots + x_{kim})^T$$

$$\equiv g^{\bar{\alpha}_i^T} (\alpha_i H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}] + \beta_{iK})^T$$

$$\equiv g^{\bar{\alpha}_i^T} (\alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]) + \lambda N)^T$$

$$20 \quad \equiv g^{\bar{\alpha}_i^T} (\alpha_i (H_1 [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}]))^T$$

$$\equiv g^{(H_i [\overrightarrow{I_{i1}}] [\overrightarrow{I_{m1}}] + \dots + H_K [\overrightarrow{I_{iK}}] [\overrightarrow{I_{mK}}])^T} \pmod{N}$$

where

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component

corresponding to vector I_{m1} for entity m ,

selected from own vector g_{it} for 1st block

25

of information specifying entity i ($t = 0$,
1, 2, ..., T);

x_{1im} = vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component
5 corresponding to vector I_{mj} for entity m,
selected from own vector s_{ij} for j'th block
of information specifying entity i (j = 2,
3, ..., K);

K_{im} is a common key generated by one entity i
10 for another entity m; and

y_{im} is sum of (K-1) components x_{jim} (j = 2, 3,
..., K), that is, $y_{im} = x_{2im} + x_{3im} + \dots$
+ x_{Kim} .

15 19. A common key generator provided at entities in
a cryptographic communications system for generating a
common key to be used in processing to encrypt plaintext
to ciphertext and in processing to decrypt ciphertext
back to plaintext, comprising:

20 storage means for storing secret keys peculiar to
said entities produced, according to computation formulas
given below, for divided specifying information resulting
from division of information specifying each of said
entities into a plurality of blocks;

25 selection means for selecting components
corresponding to divided specifying information for

opposite entities to be communicated with, from the secret keys stored; and

means for generating said common keys, according to computation formulas given below, using said components
5 so selected:

$$\overrightarrow{S_{i1}} = \alpha H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

$$\vdots \overrightarrow{S_{ij}} = \alpha H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$

$$\overrightarrow{S_{iK}} = \alpha H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

10 $\overrightarrow{g_{i0}} \equiv g^{\alpha_i - T} \overrightarrow{1} \pmod{N}$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i - T} \overrightarrow{S_{i1}} \pmod{N}$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i - T} < \overrightarrow{S_{i1}} >^2 \pmod{N}$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i - T} < \overrightarrow{S_{i1}} >^t \pmod{N}$$

15 $\overrightarrow{g_{iT}} \equiv g^{\alpha_i - T} < \overrightarrow{S_{i1}} >^T \pmod{N}$

where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i (j = 1, 2, ..., K)

20 [vector I_{ij}] is j'th divided specifying information for entity i;

vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{Mj} \times 2^{Mj}$ matrix made up of

25 random numbers;

M_j is size of j'th divided specifying
information for entity i;

K is number of block divisions in information
specifying entity i;

5 α_i is a personal secret random number for entity
i (where gcd (α_i, λ(N)) = 1 and λ(·) is
Carmichael function);

N is such that N = PQ (where P and Q are
prime);

10 β_{ij} is a personal secret random number for
entity i (where β_{i1} + β_{i2} + ... + β_{iK} =
λ(N));

g is maximum generating element with modulo N;
vector g_{it} is a secret key for 1st block of

15 information specifying entity i (t = 0,
1, 2, ..., T);

T is degree of exponent portion; and
if c is a scalar, and A and B are matrixes
represented in (i) and (ii) below, the
expressions B = c^A and B = <A>^c represent

20 (iii) and (iv) below, respectively.

$$(i) \quad A = (a_{\mu\nu})$$

$$(ii) \quad B = (b_{\mu\nu})$$

$$(iii) \quad b_{\mu\nu} = c^{a_{\mu\nu}}$$

$$(iv) \quad b_{\mu\nu} = a_{\mu\nu}c$$

$$g_{0im} = \overrightarrow{g}_{i0} [\overrightarrow{I}_{m1}]$$

$$g_{1im} = \overrightarrow{g}_{i1} [\overrightarrow{I}_{m1}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g}_{it} [\overrightarrow{I}_{m1}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g}_{iT} [\overrightarrow{I}_{m1}]$$

5

$$x_{2im} = \overrightarrow{s}_{i2} [\overrightarrow{I}_{m2}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s}_{ij} [\overrightarrow{I}_{mj}]$$

$$\vdots$$

$$x_{Kim} = \overrightarrow{s}_{iK} [\overrightarrow{I}_{mK}]$$

$$K_{im} \equiv \prod_{t=0}^T g_{tim}^T c_t y_{im}^{(T-t)}$$

10

$$\equiv g_{\alpha_i}^{-T} \sum_{t=0}^T c_x^t x_{1im}^t y_{im}^{T-t}$$

$$\equiv g_{\alpha_i}^{-T} (x_{1im} + y_{im})^T$$

$$\equiv g_{\alpha_i}^{-T} (x_{1im} + \dots + x_{kim})^T$$

$$\equiv g_{\alpha_i}^{-T} (\alpha_i H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \beta_{i1} + \dots + \alpha_i H_K [\overrightarrow{I}_{ik}] [\overrightarrow{I}_{mk}] + \beta_{ik})^T$$

$$\equiv g_{\alpha_i}^{-T} (\alpha_i H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \dots + H_K [\overrightarrow{I}_{ik}] [\overrightarrow{I}_{mk}])^T + \lambda \infty^T$$

15

$$\equiv g_{\alpha_i}^{-T} (\alpha_i H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \dots + H_K [\overrightarrow{I}_{ik}] [\overrightarrow{I}_{mk}])^T$$

$$\equiv g_{\alpha_i}^{-T} (H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \dots + H_K [\overrightarrow{I}_{ik}] [\overrightarrow{I}_{mk}])^T \pmod{N}$$

where

20

g_{tim} (= vector g_{it} [vector I_{m1}]) is a component
corresponding to vector I_{m1} for entity m ,
selected from own vector g_{it} for 1st block
of information specifying entity i ($t = 0,$
 $1, 2, \dots, T$);

25

$x_{1im} = \text{vector } s_{i1} [\text{vector } I_{m1}]$;

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component

corresponding to vector I_{mj} for entity m ,
selected from own vector s_{ij} for j 'th block
of information specifying entity i ($j = 2,$
 $3, \dots, K$);

5 K_{im} is a common key generated by one entity i
 for another entity m ; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3,$
 \dots, K), that is, $y_{im} = x_{2im} + x_{3im} + \dots$
 + x_{Kim} .

10

20. A cryptographic communications system for reciprocally performing, between a plurality of entities, encryption processing for encrypting plaintext that is information to be sent into ciphertext and decryption 15 processing for decrypting ciphertext so sent back into original plaintext, comprising:

a plurality of centers each of which generates secret keys peculiar to said entities, according to computation formulas given below, using divided 20 specifying information resulting from division of information specifying each of said entities into a plurality of blocks, and sends said secret keys to said entities; and

25 a plurality of entities each of which generates a common key mutually employed in said encryption and decryption processing when communicating with another

entity, according to computation formulas given below, using a component contained in own secret key sent from said centers, the component corresponding to divided specifying information for said another entity:

$$5 \quad \overrightarrow{S_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

$$\overrightarrow{S_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$

$$\overrightarrow{S_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i - T} \overrightarrow{1} \pmod{N}$$

$$10 \quad \overrightarrow{g_{i1}} \equiv g^{\alpha_i - T} \overrightarrow{S_{i1}} \pmod{N}$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i - T} < \overrightarrow{S_{i1}} >^2 \pmod{N}$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i - T} < \overrightarrow{S_{i1}} >^t \pmod{N}$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i - T} < \overrightarrow{S_{i1}} >^T \pmod{N}$$

where

15 vector $\overrightarrow{s_{ij}}$ is a secret key corresponding to j'th divided specifying information for entity i (j = 1, 2, ..., K)

[vector $\overrightarrow{I_{ij}}$] is j'th divided specifying information for entity i;

20 vector $\overrightarrow{1}$ is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information
specifying entity i;

α_i is a personal secret random number for entity
i (where gcd (α_i, λ(N)) = 1 and λ(·) is
5 Carmichael function);

N is such that N = PQ (where P and Q are
prime);

β_{ij} is a personal secret random number for
entity i (where β_{i1} + β_{i2} + ... + β_{ik} =
10 λ(N));

g is maximum generating element with modulo N;
vector g_{it} is a secret key for 1st block of
information specifying entity i (t = 0,
1, 2, ..., T);

T is degree of exponent portion; and
if c is a scalar, and A and B are matrixes
represented in (i) and (ii) below, the
expressions B = c^A and B = <A>^c represent
15 (iii) and (iv) below, respectively.

(i) A = (a_{μν})
(ii) B = (b_{μν})
20 (iii) b_{μν} = c^{a_{μν}}
(iv) b_{μν} = a_{μν}^c

25
30 $\mathbf{g}_{0im} = \overrightarrow{\mathbf{g}}_{i0} [\overrightarrow{I_{m1}}]$

$$g_{1im} = \overrightarrow{g}_{i1} [\overrightarrow{I}_{m1}]$$

$$g_{tim} = \overrightarrow{g}_{it} [\overrightarrow{I}_{m1}]$$

$$g_{T im} = \overrightarrow{g}_{iT} [\overrightarrow{I}_{m1}]$$

$$x_{2im} = \overrightarrow{s}_{i2} [\overrightarrow{I}_{m2}]$$

$$5 \quad x_{jim} = \overrightarrow{s}_{ij} [\overrightarrow{I}_{mj}]$$

$$x_{K im} = \overrightarrow{s}_{iK} [\overrightarrow{I}_{mK}]$$

$$K_{im} \equiv \prod_{t=0}^T g_{tim}^T C_t y_{im}^{(T-t)}$$

$$\equiv g_i^{-T} \sum_{t=0}^T C x_{1im}^t y_{im}^{T-t}$$

$$\equiv g_i^{-T} (x_{1im} + y_{im})^T$$

$$\equiv g_i^{-T} (x_{1im} + \dots + x_{kim})^T$$

$$\equiv g_i^{-T} (\alpha_i H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \beta_{i1} + \dots + \alpha_i H_K [\overrightarrow{I}_{iK}] [\overrightarrow{I}_{mK}] + \beta_{iK})^T$$

$$\equiv g_i^{-T} (\alpha_i H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \dots + H_K [\overrightarrow{I}_{iK}] [\overrightarrow{I}_{mK}])^T + \lambda \infty$$

$$\equiv g_i^{-T} (\alpha_i H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \dots + H_K [\overrightarrow{I}_{iK}] [\overrightarrow{I}_{mK}]))^T$$

$$15 \quad \equiv g_i^{-T} (H_1 [\overrightarrow{I}_{i1}] [\overrightarrow{I}_{m1}] + \dots + H_K [\overrightarrow{I}_{iK}] [\overrightarrow{I}_{mK}])^T \pmod{N}$$

where

20 g_{tim} (= vector \overrightarrow{g}_{it} [vector \overrightarrow{I}_{m1}]) is a component
corresponding to vector \overrightarrow{I}_{m1} for entity m,
selected from own vector \overrightarrow{g}_{it} for 1st block
of information specifying entity i ($t = 0,$
 $1, 2, \dots, T$);

$x_{1im} = \text{vector } s_{i1} [\text{vector } I_{m1}];$

25 x_{jim} (= vector \overrightarrow{s}_{ij} [vector \overrightarrow{I}_{mj}]) is a component
corresponding to vector \overrightarrow{I}_{mj} for entity m,
selected from own vector \overrightarrow{s}_{ij} for j'th block

of information specifying entity i (j = 2,
3, ..., K);

K_{im} is a common key generated by one entity i
for another entity m; and

5 y_{im} is sum of (K-1) components x_{jim} (j = 2, 3,
..., K), that is, $y_{im} = x_{2im} + x_{3im} + \dots$
+ x_{Kim} .

21. A computer readable recording medium for
10 storing a program that generates at entities involved in
communications a common key mutually used in processing
to encrypt plaintext to ciphertext and in processing to
decrypt said ciphertext back to said plaintext in a
cryptographic communications system, comprising:

15 first program code means for causing said computer
to select a component corresponding to divided specifying
information of one entity that is a ciphertext recipient
from a secret key peculiar to another entity that is a
ciphertext sender, according to computation formulas
20 given below, for each of divided specifying information
resulting from division of information specifying each of
said entities into a plurality of blocks; and

25 second program code means for causing said computer
to generate said common key, according to computation
formulas given below, using said components selected:

$$\overrightarrow{S}_{i1} = \alpha_i H_1 [\overrightarrow{I}_{i1}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i,2}} = \alpha_i H_2 [\overrightarrow{I}] + \beta_{i,2} \overrightarrow{1}$$

$$\overrightarrow{S_{i,j}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{i,j} \overrightarrow{1}$$

$$\overrightarrow{S_{i,K}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{i,K} \overrightarrow{1}$$

$$\overrightarrow{g_{i,0}} \equiv g^{\alpha_i^{-T}} \overrightarrow{1} \pmod{N}$$

5 $\overrightarrow{g_{i,1}} \equiv g^{\alpha_i^{-T}} \overrightarrow{S_{i,1}} \pmod{N}$

$$\overrightarrow{g_{i,2}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i,1}} >^2 \pmod{N}$$

$$\overrightarrow{g_{i,t}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i,1}} >^t \pmod{N}$$

$$\overrightarrow{g_{i,T}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i,1}} >^T \pmod{N}$$

10 where

vector s_{ij} is a secret key corresponding to j'th divided specifying information for entity i (j = 1, 2, ..., K)

[vector I_{ij}] is j'th divided specifying information for entity i;

15 vector 1 is a vector of dimension K wherein all components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of random numbers;

20 M_j is size of j'th divided specifying information for entity i;

K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity

25 i (where $\gcd(\alpha_i, \lambda(N)) = 1$ and $\lambda(\cdot)$ is

Carmichael function);
 N is such that $N = PQ$ (where P and Q are
 prime);
 β_{ij} is a personal secret random number for
 entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{ik} =$
 $\lambda(N)$);
 g is maximum generating element with modulo N;
 vector g_{it} is a secret key for 1st block of
 information specifying entity i ($t = 0,$
 $1, 2, \dots, T$);
 T is degree of exponent portion; and
 if c is a scalar, and A and B are matrixes
 represented in (i) and (ii) below, the
 expressions $B = c^A$ and $B = \langle A \rangle^c$ represent
 (iii) and (iv) below, respectively.
 $(i) \quad A = (a_{\mu\nu})$
 $(ii) \quad B = (b_{\mu\nu})$
 $(iii) \quad b_{\mu\nu} = c^{a_{\mu\nu}}$
 $(iv) \quad b_{\mu\nu} = a_{\mu\nu}^c$
 $\mathbf{g}_{0im} = \overrightarrow{\mathbf{g}_{i0}} [\overrightarrow{I_{m1}}]$
 $\mathbf{g}_{1im} = \overrightarrow{\mathbf{g}_{i1}} [\overrightarrow{I_{m1}}]$
 $\mathbf{g}_{tim} = \overrightarrow{\mathbf{g}_{it}} [\overrightarrow{I_{m1}}]$
 $\mathbf{g}_{Tim} = \overrightarrow{\mathbf{g}_{iT}} [\overrightarrow{I_{m1}}]$

30

$$x_{2im} = s_{i2} [I_{m2}]$$

$$x_{jim} = s_{ij} [I_{mj}]$$

$$x_{Kim} = s_{ik} [I_{mK}]$$

$$K_{im} \equiv \prod_{t=0}^T g_t^{Tc_t y_{im}^{(T-t)}}$$

$$5 \quad \equiv g_i^{-T} \sum_{t=0}^T c_{x_{1im}}^t y_{im}^{T-t}$$

$$\equiv g_i^{-T} (x_{1im} + y_{im})^T$$

$$\equiv g_i^{-T} (x_{1im} + \dots + x_{kim})^T$$

$$\equiv g_i^{-T} (\alpha_i H_1 [I_{i1}] [I_{m1}] + \beta_{i1} + \dots + \alpha_i H_K [I_{iK}] [I_{mK}] + \beta_{iK})^T$$

$$\equiv g_i^{-T} (\alpha_i (H_1 [I_{i1}] [I_{m1}] + \dots + H_K [I_{iK}] [I_{mK}]) + \lambda \infty)^T$$

$$10 \quad \equiv g_i^{-T} (\alpha_i (H_1 [I_{i1}] [I_{m1}] + \dots + H_K [I_{iK}] [I_{mK}]))^T$$

$$\equiv g_i^{-T} (H_1 [I_{i1}] [I_{m1}] + \dots + H_K [I_{iK}] [I_{mK}])^T \pmod{N}$$

where

15 g_{tim} (= vector g_{it} [vector I_{mi}]) is a component

corresponding to vector I_{mi} for entity m ,

selected from own vector g_{it} for 1st block
of information specifying entity i ($t = 0,$
 $1, 2, \dots, T$);

20 $x_{1im} =$ vector s_{i1} [vector I_{m1}];

x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component

corresponding to vector I_{mj} for entity m ,
selected from own vector s_{ij} for j 'th block
of information specifying entity i ($j = 2,$
 $3, \dots, K$);

25 K_{im} is a common key generated by one entity i
for another entity m ; and

y_{im} is sum of $(K-1)$ components x_{jim} ($j = 2, 3,$

$\dots, K)$, that is, $y_{im} = x_{2im} + x_{3im} + \dots$
+ x_{Kim} .

22. A computer data signal embodied in a carrier
5 wave for generating at entities involved in
communications common keys used in processing to encrypt
plaintext to ciphertext and in processing to decrypt said
ciphertext to said plaintext in a cryptographic
communications system, comprising:

10 first code segment for causing a computer to select
a component corresponding to one or more of divided
pieces of information specifying one entity from a secret
key peculiar to another entity; and
second code segment for causing said computer to
15 generate said common keys using said components selected.

23. A computer data signal embodied in a carrier
wave for generating at entities involved in
communications a common key mutually used in processing
20 to encrypt plaintext to ciphertext and in processing to
decrypt said ciphertext back to said plaintext in a
cryptographic communications system, comprising:
first code segment for causing a computer to select
a component corresponding to divided specifying
25 information of one entity that is a ciphertext recipient
from a secret key peculiar to another entity that is a

ciphertext sender, according to computation formulas given below, for each of divided specifying information resulting from division of information specifying each of said entities into a plurality of blocks; and

5 second code segment for causing said computer to generate said common key, according to computation formulas given below, using said components selected:

$$\overrightarrow{S_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{S_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

$$10 \quad \overrightarrow{S_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$

$$\overrightarrow{S_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T}} \overrightarrow{1} \pmod{N}$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T}} \overrightarrow{S_{i1}} \pmod{N}$$

$$15 \quad \overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i1}} >^2 \pmod{N}$$

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i1}} >^t \pmod{N}$$

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T}} < \overrightarrow{S_{i1}} >^T \pmod{N}$$

where

vector s_{ij} is a secret key corresponding to j'th

20 divided specifying information for entity

i ($j = 1, 2, \dots, K$)

[vector I_{ij}] is j'th divided specifying

information for entity i;

vector 1 is a vector of dimension K wherein all

25 components are 1;

H_j is a symmetrical $2^{M_j} \times 2^{M_j}$ matrix made up of random numbers;

M_j is size of j'th divided specifying information for entity i;

5 K is number of block divisions in information specifying entity i;

α_i is a personal secret random number for entity i (where gcd (α_i , $\lambda(N)$) = 1 and $\lambda(\cdot)$ is Carmichael function);

10 N is such that N = PQ (where P and Q are prime);

β_{ij} is a personal secret random number for entity i (where $\beta_{i1} + \beta_{i2} + \dots + \beta_{ik} = \lambda(N)$);

15 g is maximum generating element with modulo N; vector g_{it} is a secret key for 1st block of information specifying entity i (t = 0, 1, 2, ..., T);

T is degree of exponent portion; and

20 if c is a scalar, and A and B are matrixes represented in (i) and (ii) below, the expressions B = c^A and B = <A>^c represent (iii) and (iv) below, respectively.

25 (i) $A = (a_{\mu\nu})$

$$(ii) \quad B = (b_{\mu\nu})$$

$$(iii) \quad b_{\mu\nu} = c^{a_{\mu\nu}}$$

$$5 \quad (iv) \quad b_{\mu\nu} = a_{\mu\nu} c$$

$$g_{0im} = \overrightarrow{g}_{i0} [I_{m1}]$$

$$g_{1im} = \overrightarrow{g}_{i1} [I_{m1}]$$

$$g_{tim} = \overrightarrow{g}_{it} [I_{m1}]$$

$$g_{Tim} = \overrightarrow{g}_{iT} [I_{m1}]$$

$$x_{2im} = \overrightarrow{s}_{i2} [I_{m2}]$$

$$x_{jim} = \overrightarrow{s}_{ij} [I_{mj}]$$

$$x_{Kim} = \overrightarrow{s}_{iK} [I_{mK}]$$

$$15 \quad K_{im} \equiv \prod_{t=0}^T g_{tim}^T c_t y_{im}^{(T-t)}$$

$$\equiv g^{\bar{\alpha}_i^T} \sum_{t=0}^T c x_{1im}^t y_{im}^{T-t}$$

$$\equiv g^{\bar{\alpha}_i^T (x_{1im} + y_{im})^T}$$

$$\equiv g^{\bar{\alpha}_i^T (x_{1im} + \dots + x_{kim})^T}$$

$$20 \quad \equiv g^{\bar{\alpha}_i^T (\alpha_i H_1 [I_{i1}] [I_{m1}] + \beta_{i1} + \dots + \alpha_i H_K [I_{iK}] [I_{mK}] + \beta_{iK})^T}$$

$$\equiv g^{\bar{\alpha}_i^T (\alpha_i H_1 [I_{i1}] [I_{m1}] + \dots + H_K [I_{iK}] [I_{mK}] + \lambda N)^T}$$

$$\equiv g^{\bar{\alpha}_i^T (\alpha_i H_1 [I_{i1}] [I_{m1}] + \dots + H_K [I_{iK}] [I_{mK}])^T}$$

$$\equiv g^{\bar{\alpha}_i^T (H_1 [I_{i1}] [I_{m1}] + \dots + H_K [I_{iK}] [I_{mK}])^T} \pmod{N}$$

where

25 g_{tim} (= vector \overrightarrow{g}_{it} [vector I_{m1}]) is a component
 corresponding to vector I_{m1} for entity m ,
 selected from own vector \overrightarrow{g}_{it} for 1st block
 of information specifying entity i ($t = 0, 1, 2, \dots, T$);

x_{1im} = vector s_{i1} [vector I_{m1}];
5 x_{jim} (= vector s_{ij} [vector I_{mj}]) is a component
 corresponding to vector I_{mj} for entity m ,
 selected from own vector s_{ij} for j 'th block
 of information specifying entity i ($j = 2,$
 3, ..., K);
K_{im} is a common key generated by one entity i
 for another entity m ; and
10 y_{im} is sum of ($K-1$) components x_{jim} ($j = 2, 3,$
 ..., K), that is, $y_{im} = x_{2im} + x_{3im} + \dots$
 + x_{Kim} .